

Exhibit F



UNITED STATES ATTORNEY'S OFFICE *Southern District of New York*

FOR IMMEDIATE RELEASE
Tuesday, March 6, 2012
<http://www.justice.gov/usao/nys>

CONTACT: U.S. ATTORNEY'S OFFICE
Press Office
(212) 637-2600

FBI
Press Office
(212) 384-2100

SIX HACKERS IN THE UNITED STATES AND ABROAD CHARGED FOR CRIMES AFFECTING OVER ONE MILLION VICTIMS

*Four Principal Members of "Anonymous" and "LulzSec" Are Charged with Computer Hacking,
and a Fifth Member Pleads Guilty*

*"AntiSec" Member is Also Arrested and Charged with Stealing Confidential Information From
Approximately 860,000 Clients and Subscribers of Stratfor*

Five computer hackers in the United States and abroad were charged today, and a sixth pled guilty, for computer hacking and other crimes. The six hackers identified themselves as aligned with the group Anonymous, which is a loose confederation of computer hackers and others, and/or offshoot groups related to Anonymous, including "Internet Feds," "LulzSec," and "AntiSec."

RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," who identified themselves as members of Anonymous, Internet Feds, and/or LulzSec, were charged in an Indictment unsealed today in Manhattan federal court with computer hacking conspiracy involving the hacks of Fox Broadcasting Company, Sony Pictures Entertainment, and the Public Broadcasting Service ("PBS"). O'CEARRBHAIL is also charged in a separate criminal Complaint with intentionally disclosing an unlawfully intercepted wire communication.

HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," who also identified himself as a member of Anonymous, Internet Feds and LulzSec, pled guilty on August 15, 2011 in U.S. District Court to a 12-count information charging him with computer hacking conspiracies and other crimes. MONSEGUR'S Information and guilty plea were unsealed today. The crimes to which MONSEGUR pled guilty include computer hacking conspiracy charges initially filed in the Southern District of New York. He also pled guilty to the following charges: a substantive hacking charge initially filed by the U.S. Attorney's Office in the Eastern District of California related to the hacks of HBGary, Inc. and HBGary Federal LLC; a substantive hacking charge initially filed by the U.S. Attorney's Office in the Central District of California related to the hack of Sony Pictures Entertainment and Fox Broadcasting

Company; a substantive hacking charge initially filed by the U.S. Attorney's Office in the Northern District of Georgia related to the hack of Infragard Members Alliance; a substantive hacking charge initially filed by the U.S. Attorney's Office in the Eastern District of Virginia related to the hack of PBS, all of which were transferred to the Southern District of New York, pursuant to Rule 20 of the Federal Rules of Criminal Procedure, in coordination with the Computer Crime and Intellectual Property Section ("CCIPS") in the Justice Department's Criminal Division.

Late yesterday, JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," who identified himself as a member of AntiSec, was arrested in Chicago, Illinois and charged in a criminal Complaint with crimes relating to the December 2011 hack of Strategic Forecasting, Inc. ("Stratfor"), a global intelligence firm in Austin, Texas, which may have affected approximately 860,000 victims. In publicizing the Stratfor hack, members of AntiSec reaffirmed their connection to Anonymous and other related groups, including LulzSec. For example, AntiSec members published a document with links to the stolen Stratfor data entitled: "Anonymous LulzSec rooting you proud" on a file sharing website.

The following allegations are based on the Indictment, the Information, the Complaints and statements made at MONSEGUR's guilty plea:

Hacks by Anonymous, Internet Feds, and LulzSec

Since at least 2008, Anonymous has been a loose confederation of computer hackers and others. MONSEGUR and other members of Anonymous took responsibility for a number of cyber attacks between December 2010 and June 2011, including denial of service ("DoS") attacks against the websites of Visa, MasterCard, and PayPal, as retaliation for the refusal of these companies to process donations to Wikileaks, as well as hacks or DoS attacks on foreign government computer systems.

Between December 2010 and May 2011, members of Internet Feds similarly waged a deliberate campaign of online destruction, intimidation, and criminality. Members of Internet Feds engaged in a series of cyber attacks that included breaking into computer systems, stealing confidential information, publicly disclosing stolen confidential information, hijacking victims' email and Twitter accounts, and defacing victims' Internet websites. Specifically, ACKROYD, DAVIS, MARTYN, O'CEARRBHAIL, and MONSEGUR, as members of InternetFeds, conspired to commit computer hacks including: the hack of the website of Fine Gael, a political party in Ireland; the hack of computer systems used by security firms HBGary, Inc. and its affiliate HBGary Federal, LLC, from which Internet Feds stole confidential data pertaining to 80,000 user accounts; and the hack of computer systems used by Fox Broadcasting Company, from which Internet Feds stole confidential data relating to more than 70,000 potential contestants on "X-Factor," a Fox television show.

In May 2011, following the publicity that they had generated as a result of their hacks, including those of Fine Gael and HBGary, ACKROYD, DAVIS, MARTYN, and MONSEGUR formed and became the principal members of a new hacking group called "Lulz Security" or "LulzSec." Like Internet Feds, LulzSec undertook a campaign of malicious cyber assaults on the websites and computer systems of various business and governmental entities in the United States and throughout the world. Specifically, ACKROYD, DAVIS, MARTYN, and

MONSEGUR, as members of LulzSec, conspired to commit computer hacks including the hacks of computer systems used by the PBS, in retaliation for what LulzSec perceived to be unfavorable news coverage in an episode of the news program "Frontline"; Sony Pictures Entertainment, in which LulzSec stole confidential data concerning approximately 100,000 users of Sony's website; and Bethesda Softworks, a video game company based in Maryland, in which LulzSec stole confidential information for approximately 200,000 users of Bethesda's website.

The Stratfor Hack

In December 2011, HAMMOND conspired to hack into computer systems used by Stratfor, a private firm that provides governments and others with independent geopolitical analysis. HAMMOND and his co-conspirators, as members of AntiSec, stole confidential information from those computer systems, including Stratfor employees' emails as well as account information for approximately 860,000 Stratfor subscribers or clients. HAMMOND and his co-conspirators stole credit card information for approximately 60,000 credit card users and used some of the stolen data to make unauthorized charges exceeding \$700,000. HAMMOND and his co-conspirators also publicly disclosed some of the confidential information they had stolen.

The Hack of International Law Enforcement

In January 2012, O'CEARRBHAIL hacked into the personal email account of an officer with Ireland's national police service, the An Garda Siochana (the "Garda"). Because the Garda officer had forwarded work emails to a personal account, O'CEARRBHAIL learned information about how to access a conference call that the Garda, the FBI, and other law enforcement agencies were planning to hold on January 17, 2012, regarding international investigations of Anonymous and other hacking groups. O'CEARRBHAIL then accessed and secretly recorded the January 17 international law enforcement conference call, and then disseminated the illegally-obtained recording to others.

* * *

MONSEGUR, 28, of New York, New York, pled guilty to three counts of computer hacking conspiracy, five counts of computer hacking, one count of computer hacking in furtherance of fraud, one count of conspiracy to commit access device fraud, one count of conspiracy to commit bank fraud, and one count of aggravated identity theft. He faces a maximum sentence of 124 years and six months in prison.

ACKROYD, 23, of Doncaster, United Kingdom, DAVIS, 29, of Lerwick, Shetland Islands, United Kingdom, MARTYN, 25 of Galway, Ireland, each are charged with two counts of computer hacking conspiracy. Each conspiracy count carries a maximum sentence of 10 years in prison.

O'CEARRBHAIL, 19, of Birr, Ireland is charged in the Indictment with one count of computer hacking conspiracy, for which he faces 10 years in prison. He is also charged in the Complaint with one count of intentionally disclosing an unlawfully intercepted wire communication, for which he faces a maximum sentence of five years in prison.

HAMMOND, 27, of Chicago, Illinois, is charged with one count of computer hacking conspiracy, one count of computer hacking, and one count of conspiracy to commit access device fraud. Each count carries a maximum sentence of 10 years in prison.

DAVIS is separately facing criminal charges in the United Kingdom, which remain pending, and ACKROYD is being interviewed today by the Police Central e-crime Unit in the United Kingdom. O'CEARRBHAIL was arrested today by the Garda.

The case is being prosecuted by the U.S. Attorney's Office for the Southern District of New York. The investigation was initiated and led by the FBI, and its New York Cyber Crime Task Force, which is a federal, state and local law enforcement task force combating cybercrime, with assistance from the PCeU; a unit of New Scotland Yard's Specialist Crime Directorate, SCD6; the Garda; the Criminal Division's CCIPS; and the U.S. Attorneys' Offices for the Eastern District of California, the Central District of California, the Northern District of Georgia, and the Eastern District of Virginia; as well as the Criminal Division's Office of International Affairs.

The charges contained in the Indictment and Complaints are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

12-068

###